Real root finding for equivariant semi-algebraic systems

Cordian Riener, Mohab Safey El Din

Real root finding for equivariant semi-algebraic systems

Cordian Riener
Department of Mathematics and Statistics
UiT The Arctic University of Norway
cordian.riener@uit.no
Mohab Safey El Din
Sorbonne Université, CNRS, INRIA,
Laboratoire d'Informatique de Paris 6, LIP6, Équipe PolSys
mohab.safey@lip6.fr

June 21, 2018

Abstract

Let $\boldsymbol{R}$ be a real closed field. We consider basic semi-algebraic sets defined by n-variate equations/inequalities of s symmetric polynomials and an equivariant family of polynomials, all of them of degree bounded by $2d < n$. Such a semi-algebraic set is invariant by the action of the symmetric group. We show that such a set is either empty or it contains a point with at most $2d-1$ distinct coordinates. Combining this geometric result with efficient algorithms for real root finding (based on the critical point method), one can decide the emptiness of basic semi-algebraic sets defined by s polynomials of degree d in time $(sn)^{O(d)}$. This improves the state-of-the-art which is exponential in n. When the variables $x_1, \ldots, x_n$ are quantified and the coefficients of the input system depend on parameters $y_1, \ldots, y_t$, one also demonstrates that the corresponding one-block quantifier elimination problem can be solved in time $(sn)^{O(dt)}$.

1 Introduction

Let $\boldsymbol{R}$ be a real closed field. A *semi-algebraic set* is a subset of $\boldsymbol{R}^n$ defined by a boolean formula whose atoms are polynomial equalities and inequalities with coefficients in $\boldsymbol{R}$. In this article, we consider basic semi-algebraic sets defined as follows. Given $F = (f_1, \ldots, f_k)$ and $G = (g_1, \ldots, g_s)$ in $\boldsymbol{R}[x_1, \ldots, x_n]$, we denote by $S(F, G) \subset \boldsymbol{R}^n$ the semi-algebraic set defined by $f_1 = \cdots = f_k = 0, g_1 \geq 0, \ldots, g_s \geq 0$. These sets arise in many areas of engineering sciences such as computational geometry, optimization, robotics (see e.g. [19, 28, 63, 46]). Algorithmic problems encompass real root finding, connectivity queries, or quantifier elimination.

Such problems are intrinsically hard [13]. In the worst case, solving quantifier elimination over the reals is doubly exponential in n and polynomial in the maximum degree of the input polynomials, see [25]. This complexity is achieved by the Cylindrical Algebraic Decomposition algorithm [17]. The idea of reducing real root finding to polynomial optimization in [57] is used in [37] to obtain the first algorithm with singly exponential complexity in n. This led to improvements for the decision problem [20, 41, 49, 9], quantifier elimination [40, 8, 44] and connectivity queries [19, 21, 42, 33, 7, 55]. Later, polar varieties are introduced in [1] for the decision problem [2, 3, 54, 4, 5], for computing roadmaps [55] or polynomial optimization [39, 35, 5, 34]. Complexity bounds are then cubic in some Bézout bound as well as practically efficient algorithms.

To break this curse of dimensionality, one exploits algebraic properties of systems defining semi-algebraic sets arising in applications. This has led to improvements, for e.g. the quadratic case [6, 36], the multi-homogeneous case [15, 43] and the important case of *symmetric semi-algebraic sets*.

Let $\mathscr{S}_n$ denote the group of permutations on a set of cardinality n. This group acts on $\boldsymbol{R}^n$ by permuting the coordinates. One says that a subset of $\boldsymbol{R}^n$ is symmetric when it is closed under this action.
Let now $f \in \boldsymbol{R}[x_1, \ldots, x_n]$. One says that f is invariant under the action of $\mathscr{S}_n$ (or in short $\mathscr{S}_n$-invariant) when for all $\sigma \in \mathscr{S}_n$, $f(\sigma x) = f$ for $x = (x_1, \ldots, x_n)$. The following result summarizes the current state-of-the-art on symmetric semi-algebraic sets.

Theorem 1 ([50, 51, 65])**.** *Let $\{f, f_1, \ldots, f_s\} \subset \boldsymbol{R}[x_1, \ldots, x_n]$ be $\mathscr{S}_n$-invariant polynomials of degree at most d.*

A. *The real algebraic set $\mathrm{V}_{\mathrm{R}}(f)$ is not empty if and only if it contains a point with at most $\lfloor \frac{d}{2} \rfloor$ distinct coordinates.*
B. *The semi-algebraic set in $S \subset \boldsymbol{R}^n$ defined by $f_1 \geq 0, \ldots, f_s \geq 0$ is not empty if and only if it contains a point with at most d distinct coordinates.*

As a consequence, on input f, one can decide the emptiness of $\mathrm{V}_{\mathrm{R}}(f)$ by partitioning – up to symmetry – the set of variables $x_1, \ldots, x_n$ into $\lfloor \frac{d}{2} \rfloor$ subsets, say $\chi_1, \ldots, \chi_{\lfloor \frac{d}{2} \rfloor}$ and set $x_i = x_j$ in the input when x_i and x_j lie in the same set χ_ℓ. This way one is led to apply the aforementioned algorithms for deciding the emptiness of semi-algebraic sets to inputs involving at most $\lfloor \frac{d}{2} \rfloor$. Since the number of such partitions lies in $O(n^d)$, one finally obtains algorithms deciding the emptiness of $\mathrm{V}_{\mathrm{R}}(f)$ (resp. S) in time $n^{O(d)}$, hence polynomial time when d is fixed. The same reasoning holds for the case (B) of Theorem 1.
Of course, semi-algebraic sets defined by $\mathscr{S}_n$-invariant constraints define symmetric semi-algebraic sets but the reciprocal is not true as illustrated with the example $x_1 \geq 0, x_2 \geq 0$. A family F of constraints in $\boldsymbol{R}[x_1, \ldots, x_n]$ is said to be $\mathscr{S}_n$-invariant when for all $f \in F$ and $\sigma \in \mathscr{S}_n$, $f(\sigma x) \in F$. Note that such families of constraints defined symmetric semi-algebraic sets. It is a major and longstanding challenge to obtain algorithms that, given a $\mathscr{S}_n$-invariant family of constraints, takes advantage of the symmetry invariance to decide if it is feasible over the reals.
The goal of this article is to *generalize* the results in [50, 51, 65] to the following special situation. Let $F = (f_1, \ldots, f_k)$ and $G = (g_1, \ldots, g_n)$ be in $\boldsymbol{R}[x_1, \ldots, x_n]$ and d be the maximum degree of those polynomials. Assume that for $1 \leq i \leq k$, f_i is $\mathscr{S}_n$-invariant and that G is $\mathscr{S}_n$-equivariant, i.e., we have $G(\sigma(x)) = (g_{\sigma(i)}(x))_{1 \leq i \leq n}$ for all $\sigma \in \mathscr{S}_n$. The topical question we address is the following one. Can we decide the emptiness of the semi-algebraic set defined by $f_1 = \cdots = f_k = 0, g_1 \geq 0, \ldots, g_n \geq 0$ in time $n^{O(d)}$, i.e. polynomial in n and exponential in d? More generally, can we take advantage of equivariance for e.g. one-block quantifier elimination?
This latter question is important for a wide range of applications, in particular for the analysis of equivariant dynamical systems, which commonly appear in biology (see [60]). Those systems are of the form $\dot{\boldsymbol{x}} = \boldsymbol{f}(\boldsymbol{x}, \lambda)$ where λ is a set of parameters and $\boldsymbol{f}$ is an equivariant family of polynomials for the action of the symmetric group on the $\boldsymbol{x}$ variables and the state variables $\boldsymbol{x}$ must be non-negative (see [60, Example 2]). When analyzing the equilibrium points of such systems w.r.t. parameters λ, we are led to solve equivariant semi-algebraic systems.
Main results. We provide a positive answer to this question. More precisely, the following holds.
(i) On input F and G as above, deciding the emptiness of $S(F, G) \cap \boldsymbol{R}^n$ can be done in time $n^{O(d)}$.
(ii) On input F and G in $\boldsymbol{R}[y_1, \ldots, y_t][x_1, \ldots, x_n]$ such that F and G satisfy the above $\mathscr{S}_n$-invariance and equivariance assumptions, the quantifier elimination problem $\exists x \in \boldsymbol{R}^n \ F = 0, G > 0$ can be solved in time $n^{O(dt)}$.
This result, which generalized Theorem 1, is of particular interest on families of systems where d is fixed and n grows. They are obtained by proving that $S(F, G)$ is not empty if and only if it contains a point with at most $2d - 1$ distinct coordinates. A key ingredient to establish such a property is the use of representation theory for equivariant maps and basic results from polynomial optimization. Combining such a geometric result with efficient algorithms for real root finding or one-block quantifier elimination yields the above complexity results. More accurate complexity results (with explicit constants in the exponent) are given under some assumptions which are proved to be generic.
We also report on practical experiments illustrating that algorithms described in this paper can tackle semi-algebraic systems which are out of reach of the current state-of-the-art.

Related works. We already mentioned several previous works which led to Theorem 1. More generally, the question of using symmetry in the context of real algebraic geometry is not new. Fundamental work started with [47, 48] which study the quotient of semi-algebraic sets, which are invariant under the action of a compact Lie group. In particular, Positivstellensätze for invariant polynomials which are non-negative on invariant semi-algebraic sets are derived. This line of work is further generalized by [16] and was applied for example in [23] to the context of the moment problem. A different line of work initiated by [32] consists in exploiting symmetries in the context of sums of squares relaxations of polynomial optimization. In particular, for optimization problems which are invariant by the symmetric group, a variety of strategies are exhibited in [52]. The topology of semi-algebraic sets defined by symmetric polynomials is also easier to understand: [11, 12] derived efficient algorithms to calculate e.g. their Euler-Poincaré characteristic.
With a more algebraic flavour, computer algebra has been developed to solve polynomial systems which are invariant under the action of some groups. Approaches for this longstanding problem focus on the zero-dimensional case and aim at describing algebraically the solution set. When all equations are invariant, invariants can be used for this purpose [24, 62]. Such an approach is completed by the use of SAGBI Gröbner bases techniques [29, 64]. When the system is globally invariant, [30, 31] provides an efficient dedicated Gröbner basis algorithm (see also [59, 18] for further developments).
Structure of the paper. Section 2 recalls properties of symmetric semi-algebraic sets and explains why a direct generalization of Theorem 1 is hopeless. Section 3 provides a proof that $S(F, G)$ is not empty iff it contains a point with at most $2d-1$ distinct coordinates. Section 4 provides a description of the algorithms and the analysis of their complexity. Section 5 reports on practical performances.

2 Preliminaries

A crucial condition in Theorem 1 is that all the polynomials defining the considered semi-algebraic sets are indeed symmetric. Such an assumption is easily bypassed in the case of real algebraic sets.

Corollary 2. *Let $f_1, \ldots, f_k \in \boldsymbol{R}[X_1, \ldots, X_n]$ with $\deg f_i \leq d$ for all i. Then $\mathrm{V}_{\mathrm{R}}(f_1, \ldots, f_n)$ is not empty if and only if it contains a point with at most d distinct coordinates.*

Proof. Consider the polynomial $g := \sum_{i=1}^{k} \sum_{\sigma \in S_n} \sigma(f_i)^2$. Then we have an equality of the real varieties $\mathrm{V}_{\mathrm{R}}(g) = \mathrm{V}_{\mathrm{R}}(f_1, \ldots, f_n)$ and g is symmetric of degree $2d$ and in this situation statement (A) in Theorem 1 yields the result. □

However, in many applications the semi-algebraic set is defined by polynomials that are not themselves symmetric.
It is feasible to replace the non-invariant inequalities by a set of new inequalities which describe the same set but are invariant [16]: any symmetric semi-algebraic set defined by s inequalities can be defined with $s+1$ inequalities which are invariant by the action of the symmetric group (see also [23, 45] for a constructive approach). However, such a "symmetrization" process comes at a price: In general it will increase the degree of the polynomials drastically. We illustrate this phenomenon in the following easy example.

Example 3. *Consider the positive orthant $S := \{\boldsymbol{x} = (\mathrm{x}_1, \ldots, \mathrm{x}_n) \in \boldsymbol{R}^n : \mathrm{x}_1 \geq 0, \ldots, \mathrm{x}_n \geq 0\}$. Clearly, S is symmetric. By considering the map which sends the coordinates of $\boldsymbol{x} \in \boldsymbol{R}^n$ to the coefficients of the polynomial $h(t) := \prod_{i=1}^{n}(t - \mathrm{x}_i)$ one can prove that S is equivalently defined by $e_1(x) \geq 0, \ldots, e_n(x) \geq 0$ where e_i denotes the i-th elementary symmetric polynomial. One implication is immediate: $\boldsymbol{x} \in S$ clearly entails that $e_i(\boldsymbol{x}) \geq 0$ for $1 \leq i \leq n$. We prove the other implication by induction on n. The case $n = 1$ is clear. Now let $\boldsymbol{x} = (\mathrm{x}_1, \ldots, \mathrm{x}_n) \in \boldsymbol{R}^n$ be not in S, i.e., let one of its coordinates be negative. Besides, without loss of generality we can assume that all $\mathrm{x}_i \neq 0$ (since S has non-empty interior). We show further that this implies that there exists $1 \leq i \leq n$ such that $e_i(\boldsymbol{x}) < 0$. Clearly, in the case when exactly one coordinate of $\boldsymbol{x}$ is negative we have $e_n(\boldsymbol{x}) < 0$ and hence our claim follows. Therefore, we assume that at least two coordinates are negative. We consider the polynomial $h(t)$ as defined above. i.e., $h(t) = t^n + \sum_{i=1}^{n}(-1)^i e_i(\boldsymbol{x}) t^{n-i}$. Notice that, by construction, all roots of h are real. By Rolle's Theorem, there exists a root of its derivative $h' := \frac{\partial h}{\partial t}$*

between every two roots of h. Since h has by construction at least two negative roots, h' has a negative root. Consider $(\tilde{\mathbf{x}}_1, \ldots, \tilde{\mathbf{x}}_{n-1}) \in \boldsymbol{R}^{n-1}$ the $n-1$ roots of h' (ordered decreasingly). Since $(\tilde{\mathbf{x}}_1, \ldots, \tilde{\mathbf{x}}_{n-1})$ is not in the $n-1$ dimensional positive orthant we can apply the induction hypothesis to the case $n-1$ to infer that at least for one $j \in \{1, \ldots, n-1\}$ we have $e_j(\tilde{\mathbf{x}}_1, \ldots, \tilde{\mathbf{x}}_{n-1}) < 0$. But since h' is the derivative of h this clearly implies $e_j(\mathbf{x}_1, \ldots, \mathbf{x}_n) = \frac{1}{n-j} e_j(\tilde{\mathbf{x}}_1, \ldots, \tilde{\mathbf{x}}_{n-1}) < 0$.
Of course, the description of S with symmetric polynomials is not unique. However, it follows from the equivalence shown above that no other description with symmetric polynomials can involve only symmetric polynomials of degree smaller than n.
Indeed, suppose that $S := \{\boldsymbol{x} \in \boldsymbol{R}^n : g_1(\boldsymbol{x}) \geq 0, \ldots, g_m(\boldsymbol{x}) \geq 0\}$, where each g_i is a symmetric polynomial. It is classically known that each symmetric polynomial can be uniquely represented as a polynomial in the elementary symmetric polynomials, i.e. for each i we have a polynomial $\gamma_i \in \boldsymbol{R}[e_1, \ldots, e_n]$ such that $g_i(x) = \gamma_i(e_1(x), \ldots, e_n(x))$. Now suppose that for each i we have $\deg g_i < n$. Since the polynomials γ_i are unique and $\deg e_n = n$, it follows, that for each i we must have $\gamma_i(0, 0, \ldots, 0, t) = 0$. Consider the point $\xi := (0, 1, 2, \ldots, n-1)$. Similarly to the above reasoning, we consider a univariate polynomial $h(t) := \prod_{i=1}^n (t - \xi_i)$ (with $\xi_i = i - 1$). Note that $e_n(\xi) = 0$. Since all n roots of h are distinct, $h - \varepsilon$ has also n distinct real roots, for a small enough positive ε. Let $\zeta \in \boldsymbol{R}^n$ be one of the roots of $h - \varepsilon$. Then, $e_n(\zeta) < 0$ and thus $\zeta \notin S$. But $e_i(\xi) = e_i(\zeta)$ for all $1 \leq i \leq n-1$ and we deduce that $\gamma_j(\zeta) = \gamma_j(\xi)$ for $1 \leq j \leq m$. Hence, we get a contradiction with $\zeta \notin S$. Therefore, every representation of S in terms of symmetric polynomials must contain at least one polynomial of degree n, hence making useless Theorem 1 for algorithmic applications.

Notice that the semi-algebraic set S defined in the example above clearly contains points for which all coordinates are the same and we note the following generalization of Theorem 1 to basic convex semi-algebraic sets.

Proposition 4. *Let $S \subset \boldsymbol{R}^n$ be basic convex symmetric semi-algebraic set. Then S is not empty if and only if it contains a point for which all coordinates are equal.*

Proof. Suppose that S is not empty and let $x \in S$. Since S is symmetric, S also contains the orbit $\{\sigma(x) : \sigma \in \mathscr{S}_n\}$ of x. Since S is convex, it contains the point $y := \frac{1}{n!} \sum_{\sigma \in \mathscr{S}_n} \sigma(x)$ and clearly all coordinates of y are equal. □

Notice that the semi-algebraic set S defined in the example above contains points for which all coordinates are the same. In view of Proposition 4 it is natural to ask, to which extent it is possible to derive statements similar to Theorem 1 for symmetric semi-algebraic sets that are defined by polynomials of low degree, which are not invariant by the action of the symmetric group. The following example shows that for general semi-algebraic sets, such a generalization is not possible:

Example 5. *Let $f := \sum_{i=1}^n (x_i - i)^2$ and its $\mathscr{S}_n$ orbit which we denote by $\mathcal{F}$. Let S be the semi-algebraic set $\{x \in \boldsymbol{R}^n : \exists g \in \mathcal{F} \text{ with } g(x) = 0\}$. By construction, S is a finite set which coincides with the orbit of $\xi = (1, \ldots, n)$. Therefore, all points in S have distinct coordinates, but S is described by quadratic polynomials.*

3 Main geometric result

One way to generalize Theorem 1 to semi-algebraic sets that are $\mathscr{S}_n$-invariant but not described by symmetric polynomials is to rely on results from the theory of finite reflection groups. A finite group is called a finite reflection group, if it is generated by orthogonal reflection on a finite set of hyperplanes. These groups are extensively studied and the particular case of the symmetric group acting by permuting the coordinates falls into this framework. We refer the interested reader to [38] for more details.

Definition 6. *Let $\phi : \boldsymbol{R}^n \to \boldsymbol{R}^n$ be a morphism given by $\boldsymbol{x} \mapsto (\phi_1(\boldsymbol{x}), \ldots, \phi_n(\boldsymbol{x}))$ and let G be a finite reflection group. Then ϕ is G-equivariant if we have $g(\phi) = \phi(g(x))$ for every $g \in G$. We will write $\mathrm{Mor}_G(\boldsymbol{R}^n, \boldsymbol{R}^n)$ for the set of G-equivariant morphisms.*

We say that a sequence of polynomials of cardinality n is G-equivariant, if it defines a G-equivariant morphism.

Example 7. *Let s be a bivariate symmetric polynomial and $d \in \mathbb{N}$. The map $(\mathbf{x}_1, \mathbf{x}_2, \mathbf{x}_3) \to (\mathbf{x}_1^d + s(\mathbf{x}_2, \mathbf{x}_3), \mathbf{x}_2^d + s(\mathbf{x}_1, \mathbf{x}_3), \mathbf{x}_3^d + s(\mathbf{x}_1, \mathbf{x}_2))$ is equivariant by the action of the symmetric group $\mathscr{S}_3$.*

Let $\boldsymbol{R}[x_1, \ldots, x_n]^G$ be the ring of polynomials in $\boldsymbol{R}[x_1, \ldots, x_n]$ which are G-invariant. There is a natural action of $\boldsymbol{R}[x_1, \ldots, x_n]^G$ on the set $\mathrm{Mor}_G(\boldsymbol{R}^n, \boldsymbol{R}^n)$ by multiplication: it clearly preserves the equivariance. In other words, the equivariant morphisms form a module over $\boldsymbol{R}[x_1, \ldots, x_n]^G$. It follows from the work of Shchvartsman [58] that this module is a free module.

Theorem 8 (Shchwartsman)**.** *For any finite reflection group G the set $\mathrm{Mor}_G(\boldsymbol{R}^n, \boldsymbol{R}^n)$ is a finite $\boldsymbol{R}[x_1, \ldots, x_n]^G$-module of rank n. Furthermore, let $\psi_1, \ldots, \psi_n$ be generators of $\boldsymbol{R}[x_1, \ldots, x_n]^G$, then every equivariant morphism can uniquely be written as $f_i = \sum_{j=1}^n \frac{\partial \psi_j}{\partial x_i} s_j$ where $s_j \in \boldsymbol{R}[x_1, \ldots, x_n]^G$.*

In the sequel we will be interested in basic semi-algebraic sets that are generated by polynomials which are $\mathscr{S}_n$ equivariant in the sense of Definition 6. The general machinery developed by Shchwartsman allows in the case of $\mathscr{S}_n$ for the following corollary, which gives a convenient description of such polynomials.

Corollary 9. *Let $\{f_1, \ldots, f_n\}$ be a set of polynomials that define an $\mathscr{S}_n$ equivariant morphism and let $\deg f_i \leq d$. Then $f_i = \sum_{j=0}^d s_j \cdot x_i^j$, where $s_j \in \boldsymbol{R}[x_1, \ldots, x_n]^{\mathscr{S}_n}$ is symmetric and of degree $\leq d - j + 1$.*

Proof. It is classically known that every symmetric polynomial can be uniquely written in terms of the first n Newton sums $p_i := \sum_{j=1}^n x_j^i$. Thus, we can use these polynomials as generators of $\boldsymbol{R}[x_1, \ldots, x_n]^{\mathscr{S}_n}$ and apply Theorem 8. Since $\mathrm{Mor}_{\mathscr{S}_n}(\boldsymbol{R}^n, \boldsymbol{R}^n)$ is a free module and the polynomials $p_1, \ldots, p_n$ are algebraically independent, the degree restrictions follow at once, since we cannot have any cancellation of degrees in the representation. □

Let us denote by $A_{2d-1} \subset \boldsymbol{R}^n$ the subset of points with at most $2d-1$ distinct coordinates.

Theorem 10. *Let $F = (f_1, \ldots, f_k)$ and $G = (g_1, \ldots, g_n)$ be sequences of polynomials in $\boldsymbol{R}[x_1, \ldots, x_n]$. Let d be the maximum of $\deg(f_i)$ and $\deg(g_j)$ for $1 \leq i \leq k$ and $1 \leq j \leq n$.*
Assume that for $1 \leq i \leq k$, f_i is $\mathscr{S}_n$ invariant, that G is $\mathscr{S}_n$-equivariant and that $\deg(g_j) \geq 2$ for $1 \leq j \leq n$. Then, the basic semi-algebraic set $S(F, G)$ is empty if and only if $S(F, G) \cap A_{2d-1} = \emptyset$.

Recall that p_i denotes the Newton sum $\sum_{i=1}^n x_i^j$. For the proof of Theorem 10, we study some varieties defined by the p_i's. Let $\gamma := (\gamma_1, \ldots, \gamma_d) \in \boldsymbol{R}^d$ then we denote by $\mathscr{N}_\gamma$ the real variety

$$\mathscr{N}_\gamma := \{x \in \boldsymbol{R}^n \, : \, p_1(x) = \gamma_1, \ldots, p_d(x) = \gamma_d\}.$$

These varieties will play a crucial role for the proof of Theorem 10; the following lemma illustrates the importance of these sets.

Lemma 11. *Reusing the notations introduced above, consider a $\mathscr{S}_n$-invariant polynomial f in $\boldsymbol{R}[x_1, \ldots, x_n]$ of degree d. Then f is constant over $\mathscr{N}_\gamma$.*

Proof. Since f is $\mathscr{S}_n$-invariant, one can write it as the composition $q(p_1, \ldots, p_n)$ where q is a polynomial in $\boldsymbol{R}[u_1, \ldots, u_n]$ ($u_1, \ldots, u_n$ are new variables) and the p_i's are Newton polynomials as above. Since $\deg(f) = d$ and $\deg(p_i) = i$, one also deduces that $\deg(q, u_j) = 0$ for $d + 1 \leq j \leq n$. This implies that q lies in $\boldsymbol{R}[u_1, \ldots, u_d]$ and our claim follows immediately from the definition of $\mathscr{N}_\gamma$. □

Before going further, we first examine the possible roots of the polynomials g_j in an $\mathscr{S}_n$-equivariant system on the variety $\mathscr{N}_\gamma$.

Lemma 12. *Let $d \leq n$, $\gamma \in \boldsymbol{R}^d$. Consider $(h_1, \ldots, h_n)$ a sequence of polynomials of degree at most d in $\boldsymbol{R}[x_1, \ldots, x_n]$ which are $\mathscr{S}_n$- equivariant and $\xi = (\xi_1, \ldots, \xi_n) \in \mathscr{N}_\gamma$. Then, there exist $\{\alpha_1, \ldots, \alpha_t\} \in \boldsymbol{R}^t$ with $t \leq d - 1$ such that $h_i(\xi) = 0$ if and only if $\xi_i \in \{\alpha_1, \ldots, \alpha_t\}$.*

Proof. By Corollary 9, there exist symmetric polynomials s_i of degree at most d such that $h_i := \sum_{j=1}^{d} s_j \cdot \frac{\partial p_j}{\partial x_i}$, with $\deg(s_j) \leq d$ for all $i \in \{1, \ldots, n\}$. Since for $1 \leq j \leq d$, $\deg(s_j) \leq d$ and s_j is symmetric, it follows that the value of s_j at ξ is determined by the value of the first d Newton sums at ξ (Lemma 11). Let $\gamma_i = p_i(\xi)$ for $1 \leq i \leq d$ and $\gamma = (\gamma_1, \ldots, \gamma_d)$; besides, observe that, since $\xi \in \boldsymbol{R}^n$, we have $\gamma \in \boldsymbol{R}^d$. This implies that there exist $(b_1, \ldots, b_d) \in \boldsymbol{R}^d$ such that for all $\zeta \in \mathscr{N}_\gamma \subset \boldsymbol{R}^n$, $s_1(\zeta) = b_1, \ldots, s_d(\zeta) = b_d$. For $1 \leq i \leq n$, let us define the univariate polynomial $\tilde{h}_i = \sum_{j=1}^{d} b_j x_i^{j-1}$. As a consequence, the equality $h_i(\zeta) = \tilde{h}_i(\zeta)$ holds for all $\zeta \in \mathscr{N}_\gamma$.

Now, consider the univariate polynomial $\delta(U) := \sum_{j=1}^{d} b_j U^{j-1}$ and let $\{\alpha_1, \ldots, \alpha_t\}$ be its roots in $\boldsymbol{R}$. Since δ has degree $\leq d-1$, we have $t \leq d-1$. Observe that for every point $\xi \in \mathscr{N}_\gamma \subset \boldsymbol{R}^n$, $h_i(\xi) = 0$ iff $\tilde{h}_i(\xi) = 0$ and that $\tilde{h}_i(\xi) = \delta(\xi_i)$ where ξ_i is the i-th coordinate of ξ. In other words, $h_i(\xi) = 0$ iff $\xi_i \in \{\alpha_1, \ldots, \alpha_{t-1}\}$. □

Proof of Theorem 10. Further S denotes $S(F, G)$. Note that it suffices to show that if $S \neq \emptyset$ then there exists a point in $S \cap A_{2d-1}$. So we assume that $S \neq \emptyset$ and pick $y \in S$. We set $p_1(y) = \gamma_1, \ldots, p_d(y) = \gamma_d$ and we consider the corresponding real variety $\mathscr{N}_\gamma$ as defined above. We now take the intersection $S' := S \cap \mathscr{N}_\gamma$. Notice that $d \geq 2$ (by assumption) and hence $\mathscr{N}_\gamma$ is contained in a sphere. Thus, it follows that S' is closed and bounded. Further, we slightly abuse notation by using p_{d+1} to denote the map $x \to p_{d+1}(x)$ and its restrictions to subsets of $\boldsymbol{R}^n$. Moreover, since S' is closed and bounded, we deduce that $p_{d+1}(S')$ is closed and bounded too (see [14, Theorem 2.5.8]). Hence, we deduce that there exists $\xi = (\xi_1, \ldots, \xi_n) \in S'$ with the property that $p_{d+1}(\xi)$ is maximal among all points in S'. We claim that $\xi \in A_{2d-1}$.

Let $\{i_1, \ldots, i_\ell\}$ be the set of indices such that $g_i(\xi) = 0$ if and only if $i \in \{i_1, \ldots, i_\ell\}$. By Lemma 12 applied to $G = (g_1, \ldots, g_n)$, we deduce that there exists $\alpha = (\alpha_1, \ldots, \alpha_t) \in \boldsymbol{R}^t$ with $t \leq d-1$ such that for all $i \in \{i_1, \ldots, i_\ell\}$, we have $\xi_i \in \{\alpha_1, \ldots, \alpha_t\}$. Up to re-indexing the variables we can assume that $\{i_1, \ldots, i_\ell\} = \{n-\ell+1, \ldots, n\}$. For $i \in \{n-\ell+1, \ldots, n\}$, we denote by $\kappa(i)$ the integer such that $\xi_i = \alpha_{\kappa(i)}$. This leads us to consider the intersection of S' with the affine linear space H of $\boldsymbol{R}^n$ defined by $x_{n-\ell+1} - \alpha_{\kappa(n-\ell+1)} = \cdots = x_n - \alpha_{\kappa(n)} = 0$. We denote by S'_α the intersection of S' with the aforementioned hyperplanes.

Recall that ξ lies in S'_α and chosen to maximize p_{d+1} on S'. Then, ξ also maximizes the restriction of p_{d+1} to S'_α. Further, by construction, we have that $g_i(\xi) > 0$ for all $i \in \{1, \ldots, n-\ell\}$. This shows that there exists a ball B centered at ξ, of radius small enough such that the following holds:

(i) for $i \in \{1, \ldots, n-\ell\}$, g_i does not vanish in B;

(ii) the intersection of B with the real algebraic set defined by $f_1 = \cdots = f_k = g_{n-\ell+1} = \cdots = g_n = 0$ coincides with $S'_\alpha \cap B$.

Remark now that the real algebraic set defined by $f_1 = \cdots = f_k = 0$ contains $\mathscr{N}_\gamma$. Also, applying Lemma 12 to G, one deduces that the real algebraic set defined by $g_{n-\ell+1} = \cdots = g_n = 0$ coincides with the affine linear space H. We conclude that $S'_\alpha \cap B$ contains $\mathscr{N}_\gamma \cap H$. Besides, observe that ξ lies in $\mathscr{N}_\gamma \cap H$ and recall again that it maximizes the restriction of p_{d+1} to S'_α. We deduce that ξ maximizes the restriction of p_{d+1} to $\mathscr{N}_\gamma \cap H$.

Now, two situations may occur. Either, at ξ, the truncated Jacobian matrix associated to $(p_1, \ldots, p_d)$ obtained by considering the partial derivatives w.r.t. $(x_1, \ldots, x_{n-\ell})$ is full rank or it is not. In both cases, since $\xi = (\xi_1, \ldots, \xi_n)$ maximizes the restriction of p_{d+1} to $\mathscr{N}_\gamma \cap H$, one deduces that there exists $(\lambda_0, \ldots, \lambda_d) \in \boldsymbol{R}^{d+1} - \{\mathbf{0}\}$ such that $0 = \lambda_0 \frac{\partial p_{d+1}}{\partial x_j}(\xi) - \sum_{i=1}^{d} \lambda_i \frac{\partial p_i}{\partial x_j}(\xi)$ for $1 \leq j \leq n-\ell$. This is rewritten as $0 = (d+1)\lambda_0 \xi_j^d - \sum_{i=1}^{d} (i)\lambda_i \xi_j^{i-1}$ for $1 \leq j \leq n-\ell$. The above algebraic relation entails that for $1 \leq j \leq n-\ell$, ξ_j is a root of the non-zero univariate polynomial $\eta(U) := \sum_{i=0}^{d} \lambda_i U^i$ of degree at most d (recall that $(\lambda_0, \ldots, \lambda_d) \neq (0, \ldots, 0)$). Therefore, at most d of the first $n-\ell$ coordinates of ξ can be distinct. Further, by construction, we have that there are at most $d-1$ possibilities for the last ℓ coordinates of ξ. Therefore, $\xi \in A_{2d-1}$ as claimed. □

Remark 1. *Observe that when F is $\mathscr{S}_n$-equivariant (instead of having all of its entries $\mathscr{S}_n$-invariant), the conclusions of Theorem 10 still hold. To see that it suffices to replace F be the sum of the squares of its entries. Also when the entries of F are subject to inequality constraints (instead of equality constraints), the conclusions of Theorem 10 still hold as one can replace inequalities by equations as in [7, Chap. 13].*

4 Algorithms and complexity

4.1 Deciding emptiness

Further, we let $\boldsymbol{Q}$ be a real field, $\boldsymbol{R}$ be a real closed field containing $\boldsymbol{Q}$ and $\boldsymbol{C}$ be an algebraic closure of $\boldsymbol{R}$. We consider $F = (f_1, \ldots, f_k)$ and $G = (g_1, \ldots, g_n)$ be polynomial sequences in $\boldsymbol{Q}[x_1, \ldots, x_n]$. As above, the semi-algebraic set of $\boldsymbol{R}^n$ defined by

$$f_1 = \cdots = f_k = 0, \qquad g_1 \geq 0, \ldots, g_n \geq 0$$

is denoted by $S(F, G)$. We start with a first complexity statement.

Theorem 13. *Let F and G be as above and d be an integer bounding the degrees of the polynomials in F and G. Assume that the polynomials in F are $\mathscr{S}_n$-invariant and that the map $\mathbf{x} \mapsto (g_1(\mathbf{x}), \ldots, g_n(\mathbf{x}))$ is $\mathscr{S}_n$-equivariant and that $d \leq n/2$.*
There exists an algorithm which, on input (F, G) decides whether $S(F, G)$ is empty using at most $n^{O(d)}$ arithmetic operations in $\boldsymbol{Q}$.

Proof. By Theorem 10, $S(F, G)$ is non-empty if and only if there exists $\boldsymbol{x} \in S(F, G)$ with at most $2d - 1$ distinct coordinates.
For $\boldsymbol{x} = (\mathbf{x}_1, \ldots, \mathbf{x}_n) \in \boldsymbol{R}^n$, we denote by $v(\boldsymbol{x}) = \{v_1, \ldots, v_p\}$ (with $p \leq n$ depending on $\boldsymbol{x}$) the set of values taken by the coordinates of $\boldsymbol{x}$ and by $\mathscr{P}(\boldsymbol{x}) = (\mathscr{P}_1, \ldots, \mathscr{P}_p)$ the partition given by the sets $\mathscr{P}_j = \{x_i \mid \mathbf{x}_i = v_j\}$. Up to renumbering, one assumes that the $\mathscr{P}_i$'s are given by ascending cardinality.
Hence, set $r = 2d - 1$ and consider a partition $\gamma = [\gamma_1, \ldots, \gamma_r]$ of n of size r, i.e. $\gamma_1 + \cdots + \gamma_r = n$ with $\gamma_i \in \mathbb{N} - \{0\}$ for $1 \leq i \leq r$ and $\gamma_{i-1} \leq \gamma_i$ (by convention, $\gamma_0 = 0$). We say that a partition $\mathscr{P}_1, \ldots, \mathscr{P}_p$ of $(x_1, \ldots, x_n)$ is compatible with γ if $p \leq r$ and there exists an increasing sequence of integers s_i such that $|\mathscr{P}_i| = \gamma_{s_{i-1}} + \cdots + \gamma_{s_i}$.
We prove below that, given γ, one can decide in time $n^{O(r)}$ the existence of a real point $\boldsymbol{x}$ in $S(F, G)$ such that $\mathscr{P}(\boldsymbol{x})$ is compatible with γ. Bounding further the number of partitions of size r by n^r will establish the announced result (recall that $r = 2d - 1$).
Assume that such a point $\boldsymbol{x} = (\mathbf{x}_1, \ldots, \mathbf{x}_n)$ exists and consider $\mathscr{P}(\boldsymbol{x}) = (\mathscr{P}_1, \ldots, \mathscr{P}_p)$. For $\sigma \in \mathscr{S}_n$ we denote by $\sigma(\mathscr{P}_i)$ the set $\{x_{\sigma(j)} \mid x_j \in \mathscr{P}_i\}$. Let σ be a permutation of $\mathscr{S}_n$ such that $\sigma(\mathscr{P}_i) = \{x_{s_{i-1}}, \ldots, x_{s_i}\}$ and consider $\sigma(\boldsymbol{x}) = (\mathbf{x}_{\sigma(1)}, \ldots, \mathbf{x}_{\sigma(n)})$. Now, remark that since all entries of F are invariant by the action of $\mathscr{S}_n$ and that G is $\mathscr{S}_n$-equivariant, $\sigma(\boldsymbol{x}) \in S(F, G)$. This leads us to associate to γ the partition $\Gamma = (\Gamma_1, \ldots, \Gamma_r)$ of $(x_1, \ldots, x_n)$ defined by $\Gamma_i = \{x_{\gamma_{i-1}+1}, \ldots, x_{\gamma_i}\}$ with $\gamma_0 = 0$ by convention.
Now, let $a_1, \ldots, a_r$ be new indeterminates. Next, we perform the substitution $x_{\gamma_{i-1}+1} = \cdots = x_{\gamma_i} = a_i$ for $1 \leq i \leq r$ in F and G. In the end, one obtains polynomial families in $\boldsymbol{R}[a_1, \ldots, a_r]$. The above discussion shows that we only need to decide the existence of real points to the new system one obtains this way. Using [10,], this is done in time $n^{O(r)}$.
To finish the proof, it remains to count the number of partitions $\gamma = (\gamma_1, \ldots, \gamma_r)$ of n. The number $p(n, r)$ of partitions of n of size r satisfies the recurrence relation $p(n, r) = p(n - 1, r) + p(n - r, r)$ with $p(n, r) = 0$ if $n < r$ and $p(n, n) = p(n, 1) = 1$. A simple induction establishes the inequality $p(n, r) \leq n^r$ which finishes the proof. □

The next result establishes a more precise complexity statement: we will actually identify the constant which is in the big-Oh exponent, when the input system satisfies some properties that we will prove to be generic. Further, given a polynomial family H in $\boldsymbol{R}[x_1, \ldots, x_n]$, $V(H) \subset \boldsymbol{C}^n$ denotes the set of common solutions to H in $\boldsymbol{C}^n$.
Hence, let as above $F = (f_1, \ldots, f_k)$ and $G = (g_1, \ldots, g_n)$ in $\boldsymbol{R}[x_1, \ldots, x_n]$. Further, for $\mathcal{I} = \{i_1, \ldots, i_\ell\} \subset \{1, \ldots, n\}$, we denote by $H_{\mathcal{I}}$ the set $F \cup \{g_{i_1}, \ldots, g_{i_\ell}\}$. We say that (F, G) satisfies the assumption R when

- the jacobian matrix of F has maximal rank at all points in $V(F)$;
- for all $\mathcal{I} \subset \{1, \ldots, n\}$, the jacobian matrix of $H_{\mathcal{I}}$ has maximal rank at any point of $V(H_{\mathcal{I}})$.

Now, let r in $\{1,\dots,n\}$; we say that (F,G) satisfies assumption A_r if for any partition $\gamma=(\gamma_1,\dots,\gamma_r)$ of n, when performing the substitution $x_{\gamma_{i-1}+1}=\cdots=x_{\gamma_i}=a_i$ $(1\leq i\leq r)$ where $a_1,\dots,a_r$ are new variables in (F,G), the obtained couple of polynomial sequences (F_γ,G_γ) satisfies R.
Further, the entries of F_γ (resp. G_γ) are denoted by $f_{1,\gamma},\dots,f_{k,\gamma}$ (resp. $g_{1,\gamma},\dots,g_{n,\gamma}$). We can now state our complexity result.

Theorem 14. *Let F and G be as above in $\boldsymbol{R}[x_1,\dots,x_n]$, d be the maximum of the polynomials in F and G and E be the complexity of evaluating (F,G). Assume that for $1\leq i\leq n$, f_i is $\mathscr{S}_n$ invariant, that $\boldsymbol{g}$ is $\mathscr{S}_n$-equivariant and that $\deg(g_j)\geq 2$ for $1\leq j\leq n$ and that (F,G) satisfies assumption A_r.*
There exists an algorithm which on input (F,G) satisfying A, decides whether $S(F,G)$ is empty using $O^{\tilde{}}\left(n^{2d}(2d)^{4d+1}(pE+d^2)\right)$ arithmetic operations in $\boldsymbol{Q}$.

Proof. Further we set $r=2d-1$. By Theorem 10, $S(F,G)$ is not empty if and only if $S(F,G)$ contains a point of $\boldsymbol{R}^n$ with at most r distinct coordinates. Besides, using the invariance of (F,G) under the action of $\mathscr{S}_n$ as in the proof of Theorem 13, deciding if $S(F,G)$ contains a real point with at most r distinct coordinates can be done by deciding if at least one of the semi-algebraic sets $S_\gamma=S(F_\gamma,G_\gamma)$ is non-empty when γ ranges of the set of partitions of n of length r. We already established that the number of such partitions is upper bounded by n^r at the end of the proof of Theorem 13.
Hence, let us focus on the complexity of deciding if S_γ is empty. We need to introduce some notation. For $\mathcal{I}=\{i_1,\dots,i_\ell\}\subset\{1,\dots,n\}$, we denote by $V_{\gamma,\mathcal{I}}\subset\boldsymbol{C}^n$ the algebraic set defined by $f_{1,\gamma}=\cdots=f_{k,\gamma}=g_{i_1,\gamma}=\cdots=g_{i_\ell,\gamma}=0$. Further, we denote by $H=(h_1,\dots,h_m)\subset\boldsymbol{R}[a_1,\dots,a_r]$ these polynomials defining $V_{\gamma,\mathcal{I}}$. Further, we use linear changes of variables. Hence for $\boldsymbol{A}\in\mathrm{GL}_n(\boldsymbol{R})$, we denote by $h_i^{\boldsymbol{A}}$ the polynomial obtained by performing the change of variables $\mathbf{a}\mapsto\boldsymbol{A}^{-1}\mathbf{a}$ in h_i and by $H^{\boldsymbol{A}}$ the sequence $(h_1^{\boldsymbol{A}},\dots,h_m^{\boldsymbol{A}})$.
Using [10], we deduce that, to decide the emptiness of S_γ, it suffices to compute sample points in each connected component of the real algebraic set $V_{\gamma,\mathcal{I}}\cap\boldsymbol{R}^n$ for all $\{i_1,\dots,i_\ell\}\subset\{1,\dots,n\}$ and filter out those points which lie in S_γ. Since (F,G) satisfies A, $V_{\gamma,\mathcal{I}}$ is either empty or smooth and equidimensional of co-dimension $k+\ell$ and the above polynomial system generates a radical ideal (by the Jacobian criterion [27, Theorem 16.19]). We conclude that we only need to consider subsets of cardinality $\ell\leq r-k$. We are in position to apply the results in [54].
Actually, we use a variant of the algorithm in [54], combining the geometric approach described therein with [56]. Let π_i be the canonical projection $(\mathbf{a}_1,\dots,\mathbf{a}_r)\mapsto(\mathbf{a}_1,\dots,\mathbf{a}_i)$ and, given an equidimensional and smooth algebraic set V, let $W(\pi_i,V)$ be the critical locus of the restriction of π_i to V. We will also consider the projections $\varphi_i:(\mathbf{a}_1,\dots,\mathbf{a}_r)\mapsto\mathbf{a}_i$.
By [54, Theorem 2], in order to decide the emptiness of $V_{\gamma,\mathcal{I}}^{\boldsymbol{A}}\cap\boldsymbol{R}^n$, it suffices to perform a generic linear change of variables $\boldsymbol{A}\in\mathrm{GL}_r(\boldsymbol{R})$ and next compute rational parametrizations of all sets $\pi_{i-1}^{-1}(0)\cap W(\pi_i,V_{\gamma,\mathcal{I}}^{\boldsymbol{A}})$ for $1\leq i\leq\dim(V_{\gamma,\mathcal{I}}^{\boldsymbol{A}})+1$. Technical but immediate computations show that $\pi_{i-1}^{-1}(0)\cap W(\pi_i,V_{\gamma,\mathcal{I}}^{\boldsymbol{A}})=W(\varphi_i,Z_i)$ where $Z_i=\pi_{i-1}^{-1}(0)\cap V_{\gamma,\mathcal{I}}^{\boldsymbol{A}}$. Observe that in order to compute $Z_i=\pi_{i-1}^{-1}(0)\cap V_{\gamma,\mathcal{I}}^{\boldsymbol{A}}$ it suffices to solve the so-called Lagrange system $h_{1,i-1}^{\boldsymbol{A}}=\cdots=h_{m,i-1}^{\boldsymbol{A}}=0,[\ell_1,\dots,\ell_m]\mathsf{jac}(H_{i-1}^{\boldsymbol{A}},i)=\mathbf{0}$ where $h_{j,i-1}^{\boldsymbol{A}}$ (resp. $H_{i-1}^{\boldsymbol{A}}$) is the polynomial obtained by setting $a_1=\cdots=a_{i-1}=0$ in $h_j^{\boldsymbol{A}}$ (resp. $H^{\boldsymbol{A}}$), and $\mathsf{jac}(H_{i-1}^{\boldsymbol{A}},1)$ is the submatrix obtained by removing the first column of the Jacobian matrix associated with $H_{i-1}^{\boldsymbol{A}}$. By [55, Proposition B.1], after performing a generic linear change of variables, assumptions needed to apply [56, Theorem 16]. This latter result shows that, letting E_H be the complexity of evaluating H and $r_i=r-(i-1)$, one can solve the above Lagrange system using $O^{\tilde{}}\left(r_i^3\binom{r_i}{m}d^{2r_i+1}(pE_H+r_id+r_i^2)\right)$ arithmetic operations in $\boldsymbol{Q}$. Hence, since $\dim(V_{\gamma,\mathcal{I}})=r-m$ the total cost of computing sample points in each connected component of $V_{\gamma,\mathcal{I}}\cap\boldsymbol{R}^n$ uses $O^{\tilde{}}\left(r^4 2^{2r}d^{2r+1}(pE_H+rd+r^2)\right)$ arithmetic operations in $\boldsymbol{Q}$. Finally, observe that E_H is bounded by the complexity of evaluating the input (F,G). Also, summing up this cost to take into account all possible subsets $\mathcal{I}$ (bounded by 2^r) and the number of partitions γ (bounded by n^r) ends the proof. □

It remains to establish the genericity of assumption A. To do that, we need to define the parameters'space in which the genericity statement will hold, i.e. the space of the coefficients of (F,G) where all entries of F are $\mathscr{S}_n$-invariant and G is $\mathscr{S}_n$-equivariant (recall also that all entries of (F,G) have degree bounded by d). Let $\mathfrak{R}$ be the Reynolds operator which sends $f\in\boldsymbol{C}[x_1,\dots,x_n]$ to $\mathfrak{R}(f)=\frac{1}{n!}\sum_{\sigma\in\mathscr{S}_n}\sigma(f)$. Let now

$\mathcal{M}$ be the set of all monomials of degree $\leq d$ in $\boldsymbol{C}[x_1,\ldots,x_n]$ and $\mathcal{M}_{\mathfrak{R}} = \mathfrak{R}(\mathcal{M})$, $c = |\mathcal{M}_{\mathfrak{R}}|$ and $T_i = (t_{i,1},\ldots,t_{i,c})$ be new indeterminates for $1 \leq i \leq k$. we define now $\mathfrak{f}_i = \sum_{m_j \in \mathcal{M}_{\mathfrak{R}}} t_{i,j} m_j$ and $\mathfrak{f} = (\mathfrak{f}_1,\ldots,\mathfrak{f}_k)$ in $\boldsymbol{C}(T_1,\ldots,T_k)[x_1,\ldots,x_n]$. Observe that any sequence F such that all entries have degree bounded by d and are $\mathscr{S}_n$-invariant are obtained by specializing the indeterminates $(T_1,\ldots,T_k)$. Finally, we consider an additional sequence of indeterminates $T_{k+1} = (t_{k+1,1},\ldots,t_{k+1,c})$ a polynomial $\mathfrak{g} = \sum_{m_j \in \mathcal{M}_{\mathfrak{R}}} t_{k+1,j} m_j$. Again, any sequence G which is $\mathscr{S}_n$-equivariant is obtained as the gradient vector of a polynomial obtained by instantiating T_{k+1} in $\mathfrak{g}$. Then, we set $N = c(k+1)$ and the parameters'space we consider is $\boldsymbol{C}^N$, i.e. the one endowed by the indeterminates $(T_1,\ldots,T_{k+1})$.

Theorem 15. *There exists a non-empty Zariski open set $\mathscr{O} \subset \boldsymbol{C}^N$ such that for (F,G) in $\mathscr{O}$, (F,G) satisfies assumption* A.

Proof. Let $\mathcal{I} = \{i_1,\ldots,i_\ell\} \subset \{1,\ldots,n\}$, $r = 2d-1$, $\gamma = (\gamma_1,\ldots,\gamma_r)$ and $E_\gamma \subset \boldsymbol{C}^n$ be the linear subspace defined by $x_{\gamma_{i-1}+1} = \cdots = x_{\gamma_i}$ (for $1 \leq i \leq r$). We denote by Γ this set of linear equations which define Ext_γ. We consider the map $\Phi_{\mathcal{I},\gamma} : \boldsymbol{z} = (\boldsymbol{x},\boldsymbol{t}) \in E_\gamma \times \boldsymbol{C}^N \mapsto \left(\mathfrak{f}_1(\boldsymbol{z}),\ldots,\mathfrak{f}_k(\boldsymbol{z}),\frac{\partial \mathfrak{g}}{\partial x_{i_1}}(\boldsymbol{z}),\ldots,\frac{\partial \mathfrak{g}}{\partial x_{i_\ell}}(\boldsymbol{z})\right)$. Assume for the moment that $\mathbf{0}$ is a regular value of $\Phi_{\mathcal{I}}$. Then, the algebraic version of Thom's weak transversality theorem (see e.g. [55, Proposition B.3]) states that there exists a non-empty Zariski open set $\mathscr{O}_{\mathcal{I}}$ such that for any $\boldsymbol{t} \in \mathscr{O}_{\mathcal{I}}$, $\mathbf{0}$ is a regular value for the specialized map $\boldsymbol{x} \mapsto \Phi_{\mathcal{I}}(\boldsymbol{x},\boldsymbol{t})$. In other words, at any $\boldsymbol{x} \in \boldsymbol{C}^N$ in the zero-set of the union of Γ with $\mathfrak{f}_1(.,\boldsymbol{t}),\ldots,\mathfrak{f}_k(.,\boldsymbol{t}),\frac{\partial \mathfrak{g}}{\partial x_{i_1}}(.,\boldsymbol{t}),\ldots,\frac{\partial \mathfrak{g}}{\partial x_{i_\ell}}(.,\boldsymbol{t})$, the Jacobian matrix of that polynomial family is full rank. By the Jacobian criterion [27, Theorem 16.19], we deduce that this polynomial family satisfies R. Finally, we define $\mathscr{O}$ as the intersection of the finitely many non-empty Zariski open subsets $\mathscr{O}_{\mathcal{I}} \subset \boldsymbol{C}^N$. Hence, $\mathscr{O}$ is a non-empty Zariski open set of $\boldsymbol{C}^N$ and for any $(F,G) \in \mathscr{O}$, (F,G) satisfies A.
It remains to prove that for $\mathcal{I} = \{i_1,\ldots,i_\ell\} \subset \{1,\ldots,n\}$, $\mathbf{0}$ is a regular value of the map $\Phi_{\mathcal{I},\gamma}$, i.e. the Jacobian matrix associated to $\Phi_{\mathcal{I},\gamma}$ is invertible at any point of $\Phi^{-1}_{\mathcal{I},\gamma}(\mathbf{0})$. To do that, we prove that the Jacobian matrix associated to Γ and $\left(\mathfrak{f}_1,\ldots,\mathfrak{f}_k,\frac{\partial \mathfrak{g}}{\partial x_{i_1}},\ldots,\frac{\partial \mathfrak{g}}{\partial x_{i_\ell}}\right)$ is full rank at any point of $\Phi^{-1}_{\mathcal{I},\gamma}(\mathbf{0})$. We extract a full rank submatrix of that Jacobian matrix as follows:

- since Γ is a set of independent linear equations, one extracts a full rank square submatrix $\mathbf{J}$ with entries in $\boldsymbol{C}$ whose columns correspond to partial derivatives w.r.t. variables in $x_1,\ldots,x_n$;
- we select the columns corresponding to the partial derivatives w.r.t. indeterminates encoding the constant terms in $\mathfrak{f}_i$; this yields a diagonal submatrix Δ with 1's on the diagonal;
- we select the columns corresponding to the partial derivatives w.r.t. the indeterminate multiplying $(x_1+\cdots+x_n)$ in $\mathfrak{g}$; this yields a diagonal submatrix Δ', with 1's on the diagonal.

In the end, the submatrix we have extracted is block-diagonal and these blocks on the diagonal are $\mathbf{J}$, Δ and Δ'. This ends the proof. □

4.2 One-block quantifier elimination

We now study the situation where $F = (f_1,\ldots,f_k)$ and $G = (g_1,\ldots,g_n)$ are polynomials in $\boldsymbol{Q}[x_1,\ldots,x_n,y_1,\ldots,y_t]$ such that
(i) the action of $\mathscr{S}_n$ on $(x_1,\ldots,x_n)$ leaves invariant f_i ; *(ii)* the map $\boldsymbol{x} = (\mathbf{x}_1,\ldots,\mathbf{x}_n) \mapsto (g_1(\boldsymbol{x},.),\ldots,g_n(\boldsymbol{x},.))$ is $\mathscr{S}_n$ equivariant.
We consider the problem of computing a semi-algebraic description of the projection on the $(y_1,\ldots,y_t)$-space of the set $S(F,G) \subset \boldsymbol{R}^n \times \boldsymbol{R}^t$ defined by $f_1 = \cdots = f_k = 0, g_1 \geq 0,\ldots,g_n \geq 0$. This is equivalent to solve the one-block quantifier elimination problem:

$$\Phi : \quad \exists \boldsymbol{x} \in \boldsymbol{R}^n \quad f_1 = \cdots = f_k = 0, \quad g_1 \geq 0,\ldots,g_n \geq 0, \tag{4.1}$$

hence computing a quantifier-free formula which is equivalent to the quantified formula Φ. A geometric interpretation is that one aims at computing a semi-algebraic description of $\Pi(S(F,G))$ where Π is the projection $(\boldsymbol{x},\boldsymbol{y}) \in \boldsymbol{R}^n \times \boldsymbol{R}^t \mapsto \boldsymbol{y}$.

Theorem 16. *Let F, G and Φ be as above, d be the maximum degree in the variables in $(x_1, \ldots, x_n)$ of the entries of F and G and assume that $d \leq \frac{n}{2}$. Then, there exists a quantifier-free formula $\Psi(Y) = \cup_{k=1}^{K} \Psi_k(Y)$ which is equivalent to Φ, and such that $K \leq n^{O(d)}$ and:*

$$\Psi_k(Y) = \vee_{i=1}^{\ell_k} \wedge_{j=1}^{\ell_{i,k}} (\vee_{u=1}^{\ell_{i,j,k}} \mathrm{sign}(\varphi_{i,j,u,k}) = \sigma_{i,j,h,k})$$

$$\begin{aligned} \textit{with} \quad & \sigma_{i,j,h,k} \in \{0, 1, -1\}, \quad \ell_k \leq (n+k)^{d+1} n^{O(dt)} \\ & \ell_{i,k} \leq (n+k)^{d+1} n^{O(d)}, \quad \ell_{i,j,k} \leq n^{O(d)} \end{aligned}$$

and the degrees of the polynomials $\varphi_{i,j,u}$ are bounded by n^d. Moreover, there exists an algorithm which computes Ψ using at most $(k+n)^{dt} n^{O(dt)}$ arithmetic operations in $\boldsymbol{Q}$.

Proof. The proof is similar to the one of Theorem 13. We reduce the considered one-block quantifier elimination problem to solving finitely many one-block quantifier elimination problems.
Set $r = 2d - 1$ and let $\Gamma(n, r)$ be the set of partitions $\gamma = (\gamma_1, \ldots, \gamma_r)$ of n of size r ($\gamma_0 = 0$ by convention). As in the proof of Theorem 13, we associate to γ the substitution $x_{\gamma_{i-1}+1} = \cdots = x_{\gamma_i} = a_i$ for $1 \leq i \leq r$, where $a_1, \ldots, a_r$ are new variables. We denote by Φ_γ the formula obtained after performing this substitution in Φ and by $S_\gamma(F, G)$ the semi-algebraic set in $\boldsymbol{R}^r \times \boldsymbol{R}^t$ defined by the system obtained after applying the same substitution. Assume, for the moment, the following equality:

$$\Pi(S(F, G)) = \cup_{\gamma \in \Gamma(n,r)} \Pi(S_\gamma(F, G)). \tag{4.2}$$

Then, performing quantifier elimination on formula Φ is equivalent to performing quantifier elimination on each formula Φ_γ – which yields a quantifier-free formula Ψ_γ defining $\Pi(S_\gamma(F, G))$ – and returning $\bigvee_{\gamma \subset \Gamma(n,r)} \Psi_\gamma$. Using [10, Theorem 14.16], one deduces that performing quantifier elimination on Φ_γ is done using $(k+n)^{dt} n^{O(dt)}$ arithmetic operations in $\boldsymbol{Q}$ and it yields a formula $\Psi_\gamma(Y) = \vee_{i=1}^{\ell} \wedge_{j=1}^{\ell_i} (\vee_{u=1}^{\ell_{i,j}} \mathrm{sign}(\varphi_{i,j,u}) = \sigma_{i,j,h})$ such that $\ell \leq (n+k)^{d+1} n^{O(dt)}$, $\ell_i \leq (n+k)^{d+1} n^{O(d)}$ and $\ell_{i,j} \leq n^{O(d)}$. Now, recall that $\Gamma(n, r)$ has cardinality bounded by $n^{O(d)}$ (this bounds the integer K in the statement of the Theorem). Hence, runtime and degree bounds on the output formula are established.
Now, we prove that (4.2) holds which will end the proof. Let $\boldsymbol{y} \in \Pi(S(F, G))$ and $S_{\boldsymbol{y}} \subset \boldsymbol{R}^n$ be the projection of $S(F, G) \cap \Pi^{-1}(\boldsymbol{y})$ on the $(x_1, \ldots, x_n)$-space. Observe that $S_{\boldsymbol{y}}$ is defined by the polynomial system obtained by instantiating variables $(y_1, \ldots, y_t)$ to the coordinates of $\boldsymbol{y}$ in F and G ; we denote the obtained polynomial sequences by $F_{\boldsymbol{y}}$ and $G_{\boldsymbol{y}}$.
Observe that all entries of $F_{\boldsymbol{y}}$ are $\mathscr{S}_n$-invariant, the sequence $G_{\boldsymbol{y}}$ defines an equivariant map and all entries of $F_{\boldsymbol{y}}$ and $G_{\boldsymbol{y}}$ have degree $\leq \frac{n}{2}$ by assumption. Hence, we can apply Theorem 10. It establishes that the semi-algebraic set $S_{\boldsymbol{y}}$ is empty if and only if it contains a point $\boldsymbol{x}$ with at most $2d - 1$ coordinates. Now, observe, as in the proof of Theorem 13, thanks to the invariance of (F_γ, G_γ) that since under the action of $\mathscr{S}_n$, there exists a partition $\gamma = (\gamma_1, \ldots, \gamma_r)$ in $\Gamma(n, r)$ such that $S_{\boldsymbol{y}}$ has a non-empty intersection with the hyperplanes defined by $x_{\gamma_{i-1}+1} = \cdots = x_{\gamma_i}$ for $1 \leq i \leq r$. In other words, there exists $\gamma \in \Gamma(n, r)$ such that $\boldsymbol{y} \in \Pi(S_\gamma(F, G))$. We deduce that $\Pi(S(F, G)) \subset \cup_{\gamma \in \Gamma(n,r)} \Pi(S_\gamma(F, G))$. The reverse inclusion is immediate once we observe that $\cup_{\gamma \in \Gamma(n,r)} S_\gamma(F, G) \subset S(F, G)$. □

5 Experimental results

Our experiments make use of the following software

- RAGLIB. [53]. This is a Maple library, based on the FGB library by J.-C. Faugère. It implements algorithms based on the critical point method running in time singly exponential in n.
- MATHEMATICA-CAD [61], REALTRIANGULARIZE [22] which are packages computing Cylindrical Algebraic Decompositions (CAD) adapted to polynomial sequences.

n	d	k	**RS**	**RS-T**	**RAG**	**M**	**T**
3	2	0	1.6	8	1.6	16	6.6
4	2	0	1.9	10	13	-	-
5	2	0	4.9	9	329	-	-
6	2	0	5	25	1577	-	-
7	2	0	6	1	39461	-	-
8	2	0	10	10	-	-	-
9	2	0	10	13	-	-	-

Table 1: Results obtained for test-suite **S1**

n	d	k	**RS**	**RS-T**	**RAG**	**M**	**T**
5	3	3	1762	-	1779	-	-
6	3	3	1583	-	376822	-	-
7	3	3	3135	-	-	-	-
8	3	3	4344	-	-	-	-
5	3	4	0.4	-	0.4	-	-
6	3	4	0.4	-	21	-	-
7	3	4	0.6	-	440	-	-
8	3	4	0.9	-	11686	-	-

Table 2: Results obtained for test-suite **S2**

We have considered the following test-suites:

- **S1**. We take the gradient of randomly chosen dense symmetric polynomials for G, letting F be the empty sequence; the coefficients of these polynomials are chosen between -2^{16} and 2^{16} using the random tool generator of MAPLE.
- **S2**. We take random dense systems of symmetric polynomials and equivariant families in $\mathbb{Q}[x_1, \ldots, x_n]$.

To solve these polynomial systems, we will use the following implementations of critical point method-based algorithms and CAD:

- **RAG** refers to the Real Algebraic Geometry library RAGLIB;
- **M** refers to the CAD in MATHEMATICA;
- **T** refers to the CAD package in MAPLE.

The direct use of these polynomials will be compared with algorithms on which Theorems 13 and 14 rely. These consist in using critical point based algorithms to decide if the input system has a real solution with at most $2d-1$ distinct coordinates (where d bounds the degree of the inputs). Also we can substitute the use of those algorithms by ones that are based on CAD. This leads us to consider in our comparisons the following:

- **RS**: consists in using RAGLIB; this is an implementation of the algorithm on which Theorems 13 and 14 rely.
- **RS-T**: consists in using the CAD Maple package to look at solutions with at most $2d-1$ distinct coordinates.

The computations are performed on an Intel(R) Xeon(R) CPU E3-1505M v6 @ 3.00GHz with 32 Gb of RAM. Timings are given in seconds. The symbol '-' means that no result was obtained after 2 days of computation or because of a lack of memory. Tables 1 and 2 provide the results obtained for the test-suites **S1** and **S2**. One can see that the use of Theorem 10 allows us to tackle examples that are out of reach of other implementations.
We also observe that when $2d-1$ becomes larger than 4 or 5 implementations based on CAD cannot tackle most of the examples considered here while the critical point method based implementation RAGLIB scales far much better.

Finally, let us consider the following examples extracted from [26]:

- the problem **SWE** [26, p. 98] consists in proving that for $0 < a < b$, the semi-algebraic set defined by $m_2 > m_1^2 \frac{(a+b)^2}{4ab}, (b - x_1)(x_1 - a) \geq 0, \ldots, (b - x_n)(x_n - a) \geq 0$ is empty with

$$m_1 = \frac{1}{n} \sum_{i=1}^{n} x_i, \quad m_2 = \frac{1}{n} \sum_{i=1}^{n} x_i^2, \quad a = 1, \quad b = 2$$

- the problem 3.40.1 (referred to as **ROM**) in [26, p. 302] leads to decide the existence of real roots to the semi-algebraic system:

$$\sum_{i<j} x_i(x_i^2 + x_j^2) - \frac{1}{8} \left(\sum_{i=1}^{n} x_i \right)^4 > 0, x_1 > 0, \ldots, x_n > 0$$

The first (resp. second) table provides timings for **SWE** (resp. **ROM**). As observed previously, implementations based on the critical point methods scale way better than those based on CAD. Also our approach combined with critical point methods allows us to tackle problems which are out of reach of the state-of-the-art.

n	3	4	5	6	7	8	9
RS	0.12	0.14	0.3	0.5	0.6	0.74	1.2
RAG	0.2	0.3	0.5	1.6	9.8	131	1978
M	0.2	14.7	-	-	-	-	-

n	3	4	5	6	7	8	9
RS	0.25	0.8	4.2	95	6874	6902	14023
RAG	0.3	1	4.5	97	6664	-	-
M	0.04	0.5	1246	-	-	-	-

Cordian Riener is supported by the Tromsø Research Foundation grant 17_matte_CR. Mohab Safey El Din is supported by the ANR grant ANR-17-CE40-0009 GALOP and the PGMO grant GAMMA.

References

[1] B. Bank, M. Giusti, J. Heintz, and G.-M. Mbakop. Polar varieties and efficient real equation solving: the hypersurface case. *Journal of Complexity*, 13(1), 1997.

[2] B. Bank, M. Giusti, J. Heintz, and G.M. Mbakop. Polar varieties and efficient real elimination. *Mathematische Zeitschrift*, 238(1):115–144, 2001.

[3] B. Bank, M. Giusti, J. Heintz, and L.M. Pardo. Generalized polar varieties: Geometry and algorithms. *Journal of complexity*, 21(4):377–412, 2005.

[4] B. Bank, M. Giusti, J. Heintz, and L.M. Pardo. Bipolar varieties and real solving of a singular polynomial equation. *Jaen Journal of Approximation*, 2(1):65–77, 2010.

[5] B. Bank, M. Giusti, J. Heintz, and M. Safey El Din. Intrinsic complexity estimates in polynomial optimization. *Journal of Complexity*, 30(4):430–443, 2014.

[6] A.I. Barvinok. Feasibility testing for systems of real quadratic equations. *Discrete & Computational Geometry*, 10(1):1–13, 1993.

[7] S. Basu, R. Pollack, and M.-F. Roy. Computing roadmaps of semi-algebraic sets (extended abstract). In *STOC*, pages 168–173. ACM, 1996.

[8] S. Basu, R. Pollack, and M.-F. Roy. On the combinatorial and algebraic complexity of quantifier elimination. *Journal of ACM*, 43(6):1002–1045, 1996.

[9] S. Basu, R. Pollack, and M.-F. Roy. A new algorithm to find a point in every cell defined by a family of polynomials. In *Quantifier elimination and cylindrical algebraic decomposition*. Springer-Verlag, 1998.

[10] S. Basu, R. Pollack, and M.-F. Roy. *Algorithms in real algebraic geometry*, volume 10 of *Algorithms and Computation in Mathematics*. Springer-Verlag, 2nd edition, 2006.

[11] S. Basu and C. Riener. Bounding the equivariant betti numbers of symmetric semi-algebraic sets. *Advances in Mathematics*, 305:803–855, 2017.

[12] S. Basu and C. Riener. Efficient algorithms for computing the euler-poincaré characteristic of symmetric semi-algebraic sets. In *Ordered Algebraic Structures and Related Topics*, volume 697, page 51. American Mathematical Soc., 2017.

[13] L. Blum, F. Cucker, M. Shub, and S. Smale. *Complexity and real computation*. Springer Science & Business Media, 2012.

[14] J. Bochnak, M. Coste, and M.-F. Roy. *Real algebraic geometry*, volume 36. Springer Science, 2013.

[15] B. Bonnard, J.-C. Faugère, A. Jacquemard, M. Safey El Din, and T. Verron. Determinantal sets, singularities and application to optimal control in medical imagery. In *Proceedings of the ACM on International Symposium on Symbolic and Algebraic Computation*, pages 103–110. ACM, 2016.

[16] L. Bröcker. On symmetric semialgebraic sets and orbit spaces. *Banach Center Publications*, 44(1):37–50, 1998.

[17] C.W. Brown and J.H Davenport. The complexity of quantifier elimination and cylindrical algebraic decomposition. In *Proceedings of the 2007 international symposium on Symbolic and algebraic computation*, pages 54–60. ACM, 2007.

[18] L. Busé and A. Karasoulou. Resultant of an equivariant polynomial system with respect to the symmetric group. *Journal of Symbolic Computation*, 76:142–157, 2016.

[19] J. Canny. *The complexity of robot motion planning*. MIT Press, 1987.

[20] J. Canny. Some algebraic and geometric computations in pspace. In *Proc. of the 20-th annual ACM symposium on Theory of computing*, pages 460–467. ACM, 1988.

[21] J. Canny. Computing roadmaps in general semi-algebraic sets. *The Computer Journal*, 1993.

[22] C. Chen, J.H. Davenport, F. Lemaire, M. Moreno Maza, B. Xia, R. Xiao, and Y. Xie. Computing the real solutions of polynomial systems with the regularchains library in maple. *ACM Communications in Computer Algebra*, 45(3/4):166–168, 2012.

[23] J. Cimpric, S. Kuhlmann, and C. Scheiderer. Sums of squares and moment problems in equivariant situations. *Transactions of the American Mathematical Society*, 361:735–765, 2009.

[24] A. Colin. Solving a system of algebraic equations with symmetries. *Journal of Pure and Applied Algebra*, 117:195–215, 1997.

[25] J.H. Davenport and J. Heintz. Real quantifier elimination is doubly exponential. *Journal of Symbolic Computation*, 5(1-2):29–35, 1988.

[26] D. Djukić, V. Janković, I. Matić, and N. Petrović. *The IMO compedium. A collection of problems suggested at the International Mathematical Olympiads: 1959–2004*. Springer, 2006.

[27] D. Eisenbud. *Commutative algebra with a view toward algebraic geometry*, volume 150 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1995.

[28] H. Everett, D. Lazard, S. Lazard, and M. Safey El Din. The voronoi diagram of three lines. *Discrete & Computational Geometry*, 42(1):94–130, 2009.

[29] J.-C. Faugère and S. Rahmany. Solving systems of polynomial equations with symmetries using sagbi-gröbner bases. In *Proceedings of the 2009 international symposium on Symbolic and algebraic computation*, pages 151–158. ACM, 2009.

[30] J.-C. Faugère and J. Svartz. Solving Polynomial Systems Globally Invariant Under an Action of the Symmetric Group and Application to the Equilibria of N vortices in the Plane. In *Proceedings of the 37th International Symposium on Symbolic and Algebraic Computation*, ISSAC '12, pages 170–178. ACM, 2012.

[31] J.-C. Faugère and J. Svartz. Gröbner bases of ideals invariant under a commutative group: the non-modular case. In *Proceedings of the 38th International Symposium on Symbolic and Algebraic Computation*, pages 347–354. ACM, 2013.

[32] K. Gatermann and P.A. Parrilo. Symmetry groups, semidefinite programs, and sums of squares. *Journal of Pure and Applied Algebra*, 192(1):95–128, 2004.

[33] L. Gournay and J.-J. Risler. Construction of roadmaps in semi-algebraic sets. *Appl. Alg. in Eng. Comm. and Comp.*, 4(4):239–252, 1993.

[34] A. Greuet, F. Guo, M. Safey El Din, and L. Zhi. Global optimization of polynomials restricted to a smooth variety using sums of squares. *Journal of Symbolic Computation*, 47(5):503–518, 2012.

[35] A. Greuet and M. Safey El Din. Probabilistic algorithm for polynomial optimization over a real algebraic set. *SIAM Journal on Optimization*, 24(3):1313–1343, 2014.

[36] D. Grigoriev and D.V. Pasechnik. Polynomial-time computing over quadratic maps. *Computational complexity*, 14(1):20–52, 2005.

[37] D. Grigoriev and N. Vorobjov. Solving systems of polynomials inequalities in subexponential time. *Journal of Symbolic Computation*, 5:37–64, 1988.

[38] L.C. Grove and C.T. Benson. *Finite reflection groups*, volume 99. Springer, 1996.

[39] F. Guo, M. Safey El Din, and L. Zhi. Global optimization of polynomials using generalized critical values and sums of squares. In *Proceedings of the 2010 International Symposium on Symbolic and Algebraic Computation*, pages 107–114. ACM, 2010.

[40] J. Heintz, M.-F. Roy, and P. Solernó. Sur la complexité du principe de tarski-seidenberg. *Bulletin de la Société mathématique de France*, 118(1):101–126, 1990.

[41] J. Heintz, M.-F. Roy, and P. Solernò. On the theoretical and practical complexity of the existential theory of the reals. *The Computer Journal*, 36(5):427–431, 1993.

[42] J. Heintz, M.-F. Roy, and P. Solernó. Single exponential path finding in semi-algebraic sets II: The general case. In *Algebraic geometry and its applications*. Purdue University, West-Lafayette, 1994.

[43] D. Henrion, S. Naldi, and M. Safey El Din. Real root finding for determinants of linear matrices. *Journal of Symbolic Computation*, 74:205–238, 2016.

[44] H. Hong and M. Safey El Din. Variant quantifier elimination. *Journal of Symbolic Computation*, 47(7):883–901, 2012.

[45] E. Hubert. Invariant Algebraic Sets and Symmetrization of Polynomial Systems. working paper or preprint, April 2017.

[46] J.B. Lasserre. *Moments, positive polynomials and their applications*. World Scientific, 2009.

[47] C. Procesi. Positive symmetric functions. *Advances in Mathematics*, 29(2):219–225, 1978.

[48] C. Procesi and G. Schwartz. Inequalities defining orbit spaces. *Invenciones mathmeaticae*, 81:539–554, 1985.

[49] J. Renegar. On the computational complexity and geometry of the first order theory of the reals. *Journal of Symbolic Computation*, 13(3):255–352, 1992.

[50] C. Riener. On the degree and half-degree principle for symmetric polynomials. *Journal of Pure and Applied Algebra*, 216(4):850–856, 2012.

[51] C. Riener. Symmetric semi-algebraic sets and non-negativity of symmetric polynomials. *Journal of Pure and Applied Algebra*, 220(8):2809–2815, 2016.

[52] C. Riener, T. Theobald, L.J. Andrén, and J.-B. Lasserre. Exploiting symmetries in sdp-relaxations for polynomial optimization. *Mathematics of Operations Research*, 38(1):122–141, 2013.

[53] M. Safey El Din. Raglib (real algebraic geometry library). `http://www-polsys.lip6.fr/~safey`, 2003.

[54] M. Safey El Din and É. Schost. Polar varieties and computation of one point in each connected component of a smooth real algebraic set. In *ISSAC'03*, pages 224–231. ACM, 2003.

[55] M. Safey El Din and É. Schost. A nearly optimal algorithm for deciding connectivity queries in smooth and bounded real algebraic sets. *J. ACM*, 63(6):48:1–48:37, 2017.

[56] M. Safey El Din and É. Schost. Bit complexity for multi-homogeneous polynomial system solving application to polynomial minimization. *Journal of Symbolic Computation*, 87, 2018.

[57] A. Seidenberg. A new decision method for elementary algebra. *Annals of Mathematics*, 60:365–374, 1954.

[58] O.V. Shchvartsman. Some remarks on the chevalley theorem. *Functional Analysis and Its Applications*, 16(3):237–238, 1982.

[59] S. Steidel. Gröbner bases of symmetric ideals. *Journal of Symbolic Computation*, 54:72 – 86, 2013.

[60] I. Stewart, T. Elmhirst, and J. Cohen. *Symmetry-Breaking as an Origin of Species*, pages 3–54. Birkhäuser, Basel, 2003.

[61] A.W. Strzeboński. Cylindrical algebraic decomposition using validated numerics. *Journal of Symbolic Computation*, 41(9):1021–1038, 2006.

[62] B. Sturmfels. *Algorithms in invariant theory*. Springer Science, 2008.

[63] A. Tannenbaum and Y. Yomdin. Robotic manipulators and the geometry of real semialgebraic sets. *IEEE Journal on Robotics and Automation*, 3(4):301–307, 1987.

[64] N.M. Thiéry. Computing minimal generating sets of invariant rings of permutation groups with sagbi-grobner basis. *Discrete Mathematics and Theoretical Computer Science*, 315:328, 2001.

[65] V. Timofte. On the positivity of symmetric polynomial functions.: Part i: General results. *Journal of Mathematical Analysis and Applications*, 284(1):174–190, 2003.